Tolmie, Peter and Crabtree, Andy (2017) The practical politics of sharing personal data. Personal and Ubiquitous Computing . ISSN 1617-4917

The Practical Politics of Sharing Personal Data

PETER TOLMIE, ANDY CRABTREE, University of Nottingham

Mixed Reality Laboratory, School Of Computer Science,
University of Nottingham, Jubilee Campus, Wollaton Road, Nottingham, NG8 1BB,
United Kingdom

Email: peter.tolmie@gmail.com
Telephone: +33 677 999690

ORCID ID: 0000-0003-2548-2125

ABSTRACT

The focus of this paper is upon how people handle the sharing of personal data as an interactional concern. A number of ethnographic studies of domestic environments are drawn upon in order to articulate a range of circumstances under which data may be shared. In particular a distinction is made between the in situ sharing of data with others around you and the sharing of data with remote parties online. A distinction is also drawn between circumstances of purposefully sharing data in some way and circumstances where the sharing of data is incidental or even unwitting. On the basis of these studies a number of the organisational features of how people seek to manage the ways in which their data is shared are teased out. The paper then reflects upon how data sharing practices have evolved to handle the increasing presence of digital systems in people's environments and how these relate to the ways in which people traditionally orient to the sharing of information. In conclusion a number of ways are pointed out in which the sharing of data remains problematic and there is a discussion of how systems may need to adapt to better support people's data sharing practices in the future.

Keywords: Personal data, privacy, information sharing, domestic data management practices, ethnomethodology.

1. INTRODUCTION

The past few decades have seen a spread of digital technologies throughout our lived environments with an increasing trend towards networking those technologies such that they can interact with not just the people immediately around them but the outside world as well. Thus we now inhabit a world where increasingly large amounts of information about us, or others we know, is shared through the use of computing systems. Sometimes the process of sharing is deliberate, sometimes it is not. Sometimes the people with whom we share information are known to us, sometimes they are not. Nonetheless, across and within these systems and networks transactions are going on. 'Data'[1] is being moved between parties and that movement is somehow being managed, either by people themselves or by the systems that are handling the collection and movement of the data. So, as computing systems become an ever-more pervasive feature of our lives and are increasingly embedded in our environments through enabling platforms such as the Internet of Things, we are beginning to have to come to terms with new ways in which information relating to us might be shared or can be managed and accounted for. This has led to increasingly widespread and vocal debates regarding the implications of all of this for topics such as privacy and data confidentiality. The focus of this paper in that case is upon what happens when personal information is shared via digital means or the sharing of it is implicated by the presence of digital data of some kind. Some of this data is utterly familiar to us: it is text, or photos, or videos, etc. However, some of it is less familiar. It may concern data collected from sensors, distributed throughout households and embedded in everyday objects, such as is envisioned in many of the scenarios glossed under the notion of the Internet of Things. It may relate to ensembles of sensor data, location data and applications such as can be found in many of the health applications people use to undertake routine monitoring of health and fitness. It may relate to data collected about people's online activities, the sites they visit, with what frequency, when and where they go there, what they actually do when they are connected to a network. It may also relate to the traces left by people in the digital world as they interact with and pass through a variety of third party systems, at work, when travelling, when shopping, when undertaking cultural activities, and so on.

These digital transactions place new demands on our interactional competence. Somehow or other we are having to arrive at ways in which to manage and deal with the outcomes of this ongoing dispersal of information by digital means. At the same time, however, it is not as if these competences have arisen from nowhere. On the contrary, people have been sharing information with one another for countless eons and have a fine-tuned body of practices – what might be termed a 'practical politics'[2] – around which this sharing is articulated. It is against this backdrop of existing competence that a practical politics of sharing data is formulated. As one might expect of an arising body of reasoning, it is sometimes found wanting. But it is also rapidly evolving into a presumptive resource around which other kinds of action can be organised.

This paper makes use of a number of recent ethnographic studies of ordinary everyday life to examine what this practical politics of sharing data looks like. In particular it is going to look at some of the key organisational features of that politics: how data gets shared with others around us in our physical environment, both purposefully and incidentally; how it gets shared with remote parties, both known and unknown, through online interaction; how the sharing gets managed across all of these different situations; and how sharing practices are oriented to, reasoned about, and accounted for as a *methodical* body of practice. Along the way we shall be considering how these practices relate to how people orient to the sharing of information more broadly and accentuating the ways in which these orientations can lead to trouble when it is digital data that is being shared. Something that will be highlighted in particular is the way in which the sharing of data can breach

[1] What the Oxford English Dictionary defines as "The quantities, characters, or symbols on which operations are performed by a computer, which may be stored and transmitted in the form of electrical signals and recorded on magnetic, optical or mechanical recording media." (see https://en.oxforddictionaries.com/definition/data)

[2] The coinage of this term relates to its Greek origins and the works of Plato and Aristotle where it is associated with the active pursuit of policies to facilitate the governance of specific communities and the associated accountabilities of the governors and the governed. Here we are interested in how those policies are produced and made visible through the conduct of our everyday affairs, and how they are practically managed in our ongoing interactions *with*, and our accountability *to* specific cohorts of people.

our ordinary understandings of who might have access to information about us, with concomitant implications for how information might get premised and accounted for.

In the last few sections of the paper we shall be considering some of the specific lessons to be drawn for design out of all of this and the ways in which these lessons overturn some of the standard assumptions regarding the design of systems that might support the preservation of privacy. In conclusion we will briefly consider what future design might need to take on board to be able to effectively complement an already growing body of practice.

2. RELATED LITERATURE

The debates regarding the sharing of personal information and personal data have grown ever more vocal as computer systems have continued to extend their reach into the increasingly intimate aspects of people's lives. As a consequence the HCI literature relating to this (and the broader topic of privacy) is already vast. The following paragraphs provide a brief summary of the key perspectives that have been adopted thus far and some pointers to the primary publications. Nonetheless it should be understood that any such exercise is going to be necessarily partial and not open to being addressed properly in anything less than a full survey paper. In the discussion of the ethnographic data a number of texts will be mentioned that are more specifically related to the argument being made here.

2.1 Perspectives on the Sharing of Personal Data

2.1.1. The notion of personal data itself.

To start at the beginning, so to speak, one of the central topics addressed within the literature is what might count as personal data in the first place and then how it might be collected and handled. In relation to this a good many papers seek to somehow define personal data and its compass. So some authors draw a distinction between data that people may create themselves (e.g. emails, media, documents, etc.) and data that is created about them through the use of system logging or environmental monitoring (the role of sharing with regard to this latter point is something we shall be returning to later in this paper) [10][67]. A closely related perspective discusses distinctions between data that people may 'volunteer' to share themselves, for instance through personal profiles, applications, preferences, and posted content such as one finds on social media, and data that is surrendered to others on their behalf by human or machine-based agents [2][12][26][27][53][56][69][77]. In this vein one can also encounter a distinction being drawn between data that is actively recorded in some way and data that is simply monitored in an ongoing fashion by an infrastructure, such as lifelogging, location, or other kinds of digital traces [5][13][14]. Discussions that move beyond the point at which personal data is somehow shared and gathered may also look to the arrangements whereby the data is stored and how provision is made for its management and retrieval [14][43][67]. This is where concerns about security may also often kick in [3][4][8]. Implicit in discussions about storage are concerns about the mechanisms whereby personal data is collected in the first place and then moved to a point of storage and access. There is a weighty literature bound up with these concerns and the troubles caused by the sheer diversity and potentially distributed character of personal data, not to mention how provision may be built in to cover management and control of how the data is accessed, and even how ownership of personal data my be best defined [45][54][70]. A consideration underlying all of these perspectives that has long been generative of debate is the question of what might count as being 'personal' in the first place. Often there are attempts to treat what might be considered as being personal or sensitive as something relatively fixed [1][3], and there are a number of taxonomies and ontologies to be found in this regard [65]. But there are others who seek to challenge this view, arguing that potential sensitivity is often not considered at all [28][50] or is situationally-bound [46][54][69].

2.1.2. Methods of sharing personal data.

Another key focus in the literature that is especially pertinent for our own interests here is the ways in which personal data may be shared. Technical concerns here often centre upon the ways in which personal data might be rendered, organised, and visualized such that others may make use of it in some way [12][34][49][73]. Discussion here has also focused upon the extent to which data and data visualizations are intelligible at first encounter and how, as a consequence, people may interact with data [55]. It is noticeable that this is the least heavily populated perspective in the literature, adding to the need for the kind of endeavour being pursued in this paper.

2.1.3. Reasons for sharing personal data.

Looking beyond just the initial presentation of personal data there is also an interest in the literature regarding the underlying reasons people may have for sharing their personal data (both positive and negative), covering a loose assembly of topics such as the forging and preservation of social links [13][15][39], engendering kudos [22][26], managing identity [48][80], impression management [11], self-display [48], creating 'social capital' [26][39], maintaining trust [25][37], to preserve memories and encourage recollection [68], or even in order to facilitate various kinds of transactions, both commercial and non-commercial [24][37][53][61], and to support the provision of certain kinds of services such as healthcare [7][15].

2.1.4. The use of personal data and associated threats.

Moving on down the line from collection, comprehension, and purpose, there is an interest in how personal data may then be used by other parties, the extent to which this may constitute some kind of threat, and concomitant interests in therefore offsetting risks of inappropriate use. A lot of literature here centres upon how personal data may be used to inform things such as advertising [35][58], service development [15][30][74], product development, or direct marketing [57]. There is also some interest in how it may be used to support the identification of potential recipients of advice or instruction [42]. On the back of this come debates about the ways in which use may actual constitute misuse. The literature here is simply huge, encompassing both quite discrete topics such as the notion of attack surfaces [[9][76], and much broader ones such as privacy [6][7][8][10][13][25][30][50][51][62][69][77], consent [10][52][73], or the defamation of identity [27][48][51]. The latter may also be seen to encompass matters such as the use of personal data for the purposes of shame and ridicule, exposure, retribution, bullying, and even blackmail [32][46][69]. A deeper concern here is the extent to which people are aware of the fact their data is being used in the first place [2][5][26][33][36]. A common counterpart to discussions about privacy is once again security, this time with regard to the ways in which personal data may be revealed [16][71]. A further topic that may also be seen to be related to the preceding issues is that of onward disclosure of acquired personal data, including what might or might not be covered by legislation such as the UK's Data Protection Act [10][27][62][66].

2.2 Respecifying the interest

Whilst the above materials already constitute a rich resource across a range of topics related to the sharing of personal information, this paper is seeking to take a somewhat different tack. Instead of taking the sharing of personal data as a given and seeking to explore the implications of that, it takes as its first order of business an investigation of how the sharing of personal data is itself accomplished as a practical feature of everyday life. In other words instead of the broad-brush discussions of what is 'private' or 'personal' that typically pervade the 'privacy' literature, even in HCI, we concentrate entirely here on what notions such as 'private' or 'personal' might amount to as interactionally established matters. Whilst not dismissing the need for a range of perspectives to be adopted regarding privacy-related topics, in this paper we take the view that how privacy works as a feature of actual situated interaction is a preliminary consideration and that it is hard to fully unpack other matters if you don't have a grasp of what things like the sharing of personal data itself looks like in practice. As will be seen in all that follows, it is a multifaceted affair, with numerous subtle nuances that even here can only be dipped into rather than covered in comprehensive detail. However, it is also clear that a number of the findings outlined above make greater sense once one understands the practices underlying them. This paper is therefore not so much seeking to overturn

the edifice of existing literature on this topic as to set it on a sounder footing by articulating the interactional dynamics upon which many of the phenomena described are founded.

It should also be noted that this paper is a companion piece to a number of other articles that have been published in recent years. One such article examines the social and relational aspects of how people interact with data, with a special eye to how personal data may get articulated [18]. Another looks at how people work with, render intelligible, and account for sensor traces of their own activity [75]. Crabtree and Mortier [19] examine how the processing of personal data in the context of the Internet of Things may be resulting in a shift in where matters such as agency and control may be said to operate and, in a related paper, Crabtree et al [20] look at how new developments in how personal data may be managed could be giving rise to a 'new economic actor'. More recent papers still in the process of publication have looked at how people go about managing digital privacy in practice [21] and how digital technology may be bringing about new forms of observability and concomitant accountability in domestic environments [31]. It will also be seen that this paper builds upon an earlier paper regarding how people collaboratively work up and draw upon policies regarding the use of their home networks [17]. Where this paper sits in relation to all of these other publications is in providing a study of some of the interactional 'glue' that these various other considerations turn upon.

3. A 'DEFENSIVELY DESIGNED STORY'

As a preliminary to looking at the ethnographic work we are going to take a brief look here at a classic text by Harvey Sacks dating from the early 1970s. What the text demonstrates is the amount of subtlety and sophistication involved in sharing personal information with other people regarding the relationship that exists between the parties, their respective accountabilities and potential rights and obligations, and the role that sharing information can play in reflexively shaping how those rights and obligations might pan out in the future. Here is the short snippet of interaction that Sacks was working with:

Louise: One night- (1.0) I was with this guy that I liked a real lot. An' uh (3.0) we had come back from the show, we had gone to the (1.0) Ash Grove for a while, 'n we were gonna park. An' I can't stand a car. 'n he // has a small car.
Ken: Mm hm,
Louise: So we walked to the back, an' we just wen' into the back House an' we stayed there half the night. (1.0) We didn't go to bed to- t'each other, but- it was so comfortable an' so // nice.
Ken: Mm hm,
Ken: Mh
Louise: Y'know? There's everything perfect.

[64]

In his discussion of this story Sacks points to a number of features that lead to him describing it as what he calls a 'defensively designed' story. Clearly the account provided in this story is recognizably personal in its character and what Sacks is keen to point out is that a) this kind of story cannot just be told to anyone in any circumstance, and b) the exact way it is worked up is very tightly managed with regard to just whom it is being told to. The general term Sacks uses for such particular presentations of talk is 'recipient design', but recipient design can gloss a wide range of quite distinct phenomena so just saying the story is recipient designed is not enough. The question is just how it's recipient designed and just what kind of work that design is doing.

The background Sacks provides regarding this story is that the talk is currently about 'variant places for sex' and is being told to an unmarried male colleague. The latter fact is something Sacks focuses on in particular because his argument is that the story is defensively designed because the recipient is male, of a similar age, and unmarried. So a risk here is that the recipient might think that she is telling him about her availability. Sacks suggests that, this being the case, there are features within the telling that make it clear to Ken that, because this happened in the past, it cannot be safely read as saying anything much about what she might be willing to do now. He also points to how the use of tense within the story and the positioning of what might be referring to sex within it quite

carefully situates the sex as being a normal and expectable occurrence that just anyone of a similar age and circumstance to her might recognize. At the same time, because the talk here is about variant places for having sex, the story works to make this a recognizable variant in that the usual place for teenagers to have sex is in their cars, and so she has to make the rejection of that possibility visible. But having made that difference visible she also quite carefully says what she didn't do so that the recipient can't take it to signify much. And, as Sacks points out, she would not necessarily have seen this kind of organization of the story as being necessary had she been telling it to a girlfriend instead.

So what we can see here is that whilst people will find occasion to reveal to others really quite intimate details about their lives, they exercise very tight control, *through the mechanics of just how those details are revealed*, over just what may be made of those details – just what use may be made of the information that is being shared. As Sacks observes:

> *"... in that she's telling a rather dangerous story, its size has to do with the warding off of inferences that could be made from the specific event that she intends to tell of"* [64: Vol II, 457].

He further observes – and this is critical for our interests here:

> "*And one can see that, as complicated as it turns out to be to tell this story to even a colleague, what a job is involved if one is trying to tell it to someone who isn't. She couldn't, then, use the positioning, place, etc., the sense of "half the night," in order to bring off precisely what she's bringing off and defending against"* [ibid].

It's worth pointing out that it is also the case here that Louise's account provides for ways in which Ken might be called to account for handling the information it reveals. It is not as if Ken has received on his computer a video recording of the possible sexual encounter Louise has been telling him about and now has to work out what he might or might not do with that information or what it might tell him about her sexual availability. Her account quite neatly ties up such matters and, to all intents and purposes, tells him how he might proceed.

The purpose of presenting the above material is to bring to the fore the point that *all* witting information sharing is somehow recipient designed. This is not our discovery, of course, and the mechanics of this were best elaborated by Sacks in this account. The 'defensive' character of the story here also serves to underscore the fact that when information is shared *unwittingly* it removes the scope to design the sharing to fit the need. This is a potential risk when sharing data and this paper is a working through of how the sharing of *data* is accomplished, how the sharing is managed (which reflects Sacks's point), and how the risk is offset or, when realised, how prospective trouble is handled, when possible, through repair.

4. STUDYING THE SHARING OF DATA

This paper draws upon a collection of studies that have been undertaken over recent years and that have each, in some way, intercepted aspects of people's lives that might be deemed 'personal' or 'private'. Many, though not all, have focused upon domestic environments. The studies that are focused upon in particular fall into two principal blocks: 1) studies of the use of wireless networks in the home which have examined how online activity is interleaved with, and a feature of, ordinary everyday life (see most notably the UK EPSRC-funded project 'Homework'[3] and the European Commission funded project 'User-Centric Networking'[4]); 2) studies bound up with the notion of 'the internet of things' that have been looking at things like the explicit use of sensors to capture aspects of people's activity (see, for instance, the RCUK Digital Economy-funded project 'The Hub of All Things'[5]) or how people interact with and account for the data arising from digital traces of the things they do (see, for instance, the EPSRC-funded fellowship 'Building Accountability into

[3] homenetworks.ac.uk
[4] https://usercentricnetworking.eu
[5] hubofallthings.com/main/

the Internet of Things'[6]). Together these studies amount to a substantial body of empirically gathered materials that span about 10 years of situated observation and all of them are replete with details of how people manage and share personal information and personal data as an ordinary feature of their everyday lives.

All of the studies mentioned were ethnomethodological in character [29] and all of them hinged upon the use of ethnography. In other words they all involved situated observation of exactly how people accomplish their everyday affairs as they go about them. These observations are recorded in fine-grained detail and worked up into 'thick descriptions' [63] of just how specific activities are accomplished. The recorded elements themselves are typically assemblies of a variety of things including notes captured during the direct observations, audio recordings and video recordings captured both during the in situ accomplishment of ordinary everyday activities and during interviews, photographs and printed documents, and, in most cases, data extracted from computer-based logs. The methodological aspects of these activities are then explicated to make visible their orderly and accountable characteristics. This approach, sometimes glossed as ethnomethodologically-informed ethnography [38], has become an increasingly important aspect of systems design and is now a recurrently visible part of the design cycle in a number of communities such as Computer-Supported Cooperative Work (CSCW) and Human-Computer Interaction (HCI).

More specific details of the studies will be provided in the course of presenting various examples so that the reader can grasp more easily the context in which the recorded phenomena were observed.

5. THE SHARING OF PERSONAL DATA

There is a fundamental observation to emphasise here as the backdrop to the discussion that will be engaged in regarding the exercise of a *practical politics* when sharing data. There are now numerous ethnomethodological studies of everyday domestic life and they all explicate in detail ways in which household life is socially organized and possessed of accountable characteristics towards which members of a household are continually oriented throughout the accomplishment of their everyday affairs. This social order constitutes a *moral* order. That is, it is an order upon which the very need for explicit account or otherwise is founded. It is an order that provides for seeing what needs to be done or left alone entirely. It is an order that provides for seeing what one's rights and obligations might be and for seeing what might or might not be reasonably expected of others. As Garfinkel expressed the matter:

> *"A society's members encounter and know the moral order as perceivedly normal course of action – familiar scenes of everyday affairs, the world of daily life known in common with others and with others taken for granted"* [29: 35]

Thus when we look at the sharing of personal data there is in the same way a locally oriented to moral order that provides for what accountably appropriate sharing might look like. This order is organized around two somewhat overlapping but largely distinct concerns: how personal data is being shared with others around you who also physically share the same setting; and how personal data is being shared with other parties whose principal source of access to it is through what is made visible online. The discussion here is therefore organized around these two concerns. Within them we shall also be looking at: just how personal data sharing is managed in everyday practice; what is being oriented to within those practices – the practical politics so to speak; and, in addition, the ways in which the current design of computing systems may result in breaches of those orientations, resulting in a need for some kind of repair.

[6] iotdatabox.com/IoT/Home.html

5.1 Sharing personal data with those around you

5.1.1 Managing how the data is shared

A great deal of what people would readily describe as the sharing of personal data is currently taking place within the confines of well-understood relationships and expectable cohorts of recipients. In the following a study participant in his early 60s who had been asked to maintain and share the output of various sensors in his home, describes some of the ways in which he is already routinely sharing his health data which is collected by a fitbit and then kept and displayed on his smartphone:

> The cycling club are very concerned with their health. We're cycling with a group of older people but they're very fit. But they largely have some sort of heath problem. So there's a great discussion, when we're together, about health problems on a quite deep level because they're interested and they know their bodies … For coffee, we cycle, we stop, and at those social gatherings in between we would be sitting round a table and say well how are you and how are you and how are you? And that's when that sort of sharing takes place…to some people you might get out your phone and it becomes quite personal sharing … Depends who you're talking to.

There are a number of things to notice about this. First of all, there are appropriate places where such sharing of data can occur, e.g. sat around the table at the coffee shop rather than by the roadside, whilst cycling along, or whatever. Then there are appropriate times: whilst taking a pause when out cycling rather than when they first meet up and set off, for instance. It's also clear there are appropriate recipients for this kind of data. They are members of the cycling club. Others amongst them use the same kinds of devices and keep the same kind of data. They can be presumed to be able to reason about the data in the same kinds of ways and to therefore have a grasp of what your data is saying and what might be made of it. Clearly you could not just sit down with anyone to have coffee and make the same kinds of assumptions. Another feature worth pointing out is the way the participant says: "we would be sitting round a table and say well how are you and how are you and how are you? And that's when that sort of sharing takes place". What this recognises is that sharing personal data in this way is something that does not happen as a matter of course. It has to be occasioned, for instance through enquiries into the state of people's health. So another organisational feature people are oriented to here is the need to actually build the sharing of data into an ongoing course of interaction, using a range of mundane but recurrently visible everyday practices for doing that, such as topic raising. Another thing is understanding what an appropriate response to a question like 'how are you?' might look like. For many it might be something like 'oh, alright, bit of a cough at the moment but nothing serious'. But here, amongst this specific cohort, another appropriate response can be getting out your phone and showing people specific details like your weight, your heart rate, your blood pressure, your BMI, your body fat percentage, and so on. So there are some other methodological matters involved here regarding understanding that in certain circumstances an appropriate response to someone asking after your health might be the actual display of personal data on a device. Clearly this is not independent of a specific cohort and its interests and what is commonsensically known about that cohort. But it is also the case that ordinary questions are not typically productive of extraordinary responses, or at least not without some special kind of an account. So actively sharing personal data via the screen on a mobile phone can be a wholly routine and mundane occurrence given the right time, the right place, the right occasioning and the right cohort.

It's not that the organizational arrangements outlined above are fixed and never subject to variance. Of course they are, but in each case the appropriateness or otherwise of the sharing is commonsensically available to both the people doing the sharing and their recipients. The study participant here could send a screenshot of the health app on his phone to one of his cycling buddies whilst at work, but his cycling buddy would clearly need some further account than just the data itself to understand why it is he might be doing this. Similarly, the cycling buddy might just call him up and ask him to send him his latest data, but again the need for some further account is apparent. This underscores an important point about all of this straight away. It is not just that the sharing of personal data is open to the exercise of control by the person doing the sharing of the data. It is also the case that the practices of sharing across all of the dimensions mentioned and maybe more are ones that have to be mutually seen to be appropriate. In other words, recipients play an important

role in what data sharing practices look like. The practical sharing of personal data is an *intersubjective accomplishment*.

A thing to point out about all of this is that, when it is a party to whom the personal data refers that is doing the sharing many aspects of how the sharing gets done are tightly aligned with the observations discussed earlier that were originally made by Sacks. That is: the revelation of personal information here is very tightly tied to the mechanics of just how that information is revealed over the course of situated interaction. The active sharing of personal data is shaped and adapted in mutually accountable ways to the specific circumstances in which it is shared, and it is through what is said and not said, what is shown and not shown, what time and place is chosen or not chosen, what potential prompt is taken up or set aside, that people exercise control over what data is shared and what use may be made of it.

5.1.2 Controlling who gets to look

A way of controlling the personal data one shares with other people in situ is to control access to the device on which the data may be displayed. One might give them device, and, of course, there are occasions when this happens, but an alternative method is to show them just exactly what you want to show them on the device yourself. This is clearly a part of how the sharing was being done in the preceding example of sharing health data amongst members of a cycling club. It also came up on a number of occasions during interviews with people regarding the digital privacy management practices. It was noted to be a particularly key strategy where people wanted to share very specific content but where the content was a feature of activities and repositories that were actively described as being 'private'. Here a 21 year-old student is talking about how she might occasionally share content with others around her on Tumblr:

Evelyn: I don't like anybody seeing what's going on on Tumblr. Occasionally I'll show Susan [her sister] a- a picture or a gif of a cat. But I don't-
Fieldworker: But that's you specifically have that image and you show it to her
Evelyn: And show it to her, yeah
Fieldworker: Rather than you let her watch you doing the posting
Evelyn: Yeah

So, as a matter of method, the sharing of personal data can be accomplished by displaying it first of all on some specific device and then physically taking the device to the recipient and holding it in such a way that the recipient can see it. There are a number of permutations whereby this can be brought about. It might be that the prospective recipient is an adjacent position and it is just a matter of locating the thing to be shared and then re-angling the device so that they can see it. It may also be the case that the device is not mobile, in which case sharing may involve calling the recipient over to the device. Locating the data may also be something that is done prior to display or once the recipient is actually co-present. Reflection on these different possibilities will make an important part of all this apparent: the location of the data, its physical display, and the actual work done with the data in terms of premising it, referring to it, and then removing it from view are all things that are embedded in some ongoing course of interaction. The interaction may be something that precedes the sharing of data, with the data being drawn upon to further fuel that interaction in some sense, such as is the case when sat drinking coffee and showing round health data on your smartphone. But it may also be initiated in relation to the sharing of the data, where the relevance/interest of the data itself serves as an account for why it is being shared, such as might be the case with a specific message or image being shown to family or friends. These features of occasioning and accountability are critical aspects of how the co-present sharing of personal data might be accomplished.

5.1.3 In the course of living

Something to note about the sharing of personal data is that, in the ordinary course of living together, much of what people might know of one another is readily available through their sharing of the

same environment. However, personal *data* is often tied up within people's individual devices and it is not always just there to be seen. So in certain circumstances personal data may become specifically reportable to others in the home. In one home that was studied the husband and wife had each recently acquired a Withings Pulse, capable of recording things like the number of steps taken, distance covered, etc., as well as a Withings Smart Body Analyzer, which is basically a bathroom scales that can measure other things such as body fat. They had taken to reporting readings from the scales to one another the first time they saw each other after they had taken their weight. They would also recurrently report the number of steps and distance covered shown on their Pulse throughout the day, e.g. "I've still only done seven thousand" or "Hooray, I've reached my target" (which is ten thousand as a default). On top of this they would, as a matter of habit, review their performance in the evening, just before they went to bed, by using a Withings application on their iPad. Here is one such case:

It is late in the evening and Maud and Simon have just finished watching TV together. Maud picks up her iPad from the table, goes to Google Chrome, and does an image search for 'castle cakes' in preparation for a cake she has to make the following day. She works through saving a few images then goes out of Chrome and open the Withings application. She and Simon look at her stats together.

Maud: I haven't done much today

She clicks on the sleep display and works back through from the current day, displaying one day at a time

Simon: Why does it say zero there?
Maud: I forgot to put it on [her pulse]

Maud goes back to looking at her weight

Maud: Heh. Even my ideal weight [70] is above the blue area. For that it would have to be down to 69.
Simon: Can I see my figures?

Maud clicks back to the menu and selects Simon instead

Simon: It often fails to register my heart rate [there is no measure for the current day]. My weight is going up as well. Why is there no blue area for me?
Maud: Because you haven't set a weight target

Maud clicks out of the Withings app and goes to Chrome again and opens her Facebook page…

There are a number of things to note about this. First of all, the sharing of this information with each other has become a matter of routine, with it happening at specific points within the overall accomplishment of everyday life, and with neither of them bringing into question the fact that the other party is reporting such information. Nor is it treated as a matter for comment that one of them should open up their iPad and make such information available in doing so, or that the other should take an interest in the information and pass comment upon it. As noted above it is also the case here that the data *is* seen to be worthy of report and, again, it is not treated as strange that such reports should be forthcoming. Indeed, the points of occasioning and accountability mentioned above are covered by these things being taken to be self-evidently newsworthy. However, something to bring to particular attention here is the way that the use of the iPad means that data is made visible to the other party in an incidental fashion as part of a collection of nightly practices that are all made unproblematically visible, including browsing on the internet and looking at Facebook. The right of one party (the husband) to see the other party (the wife)'s data is presumed by both of them, and vice versa. Thus a good deal of 'data' is oriented to as stuff you would routinely share with your partner in any case and, because this shareable data is rendered *opaque* by its capture with digital devices, the opaqueness is repaired through ordinary practices of making it visible, be that through explicit account or by looking at the data on a device when the other party is going to be able to see it as well. Indeed, should one or other of them take measures to avoid revealing this kind of data the very act of trying to keep it hidden would itself become accountable. How, for instance, would it be if one evening the wife were to say: "are you off to bed now?" *before* opening her Facebook page. Thus, as with many other things, the in situ sharing of personal data is often an incidental feature of everyday life, encompassed within the pursuit of everyday routine practices rather than always being the subject of explicit forms of sharing such as those outlined above.

5.1.4 The local sharing of third party data

A further refinement of the above relates to how personal data that is not your own but rather something that has been already shared with you is then shared with other people. Consider the following:

Samantha: Erm It's weird in that sense coz I wouldn't mind somebody seeing something that I was sending, but I'd be uncomfortable about somebody seeing something that Tom [her brother] had sent me
Fieldworker: Okay. Why's that?
Samantha: It would feel like more of a breach of privacy because it is something he's sending specifically to me Often it is just like photos of him and Rick [Tom's partner] or food that he's made or things… that he's seen that reminded him of me and things like that. And it would feel much weirder for somebody to see what he was sending me than-
Fieldworker: Why would it feel weird? What would feel wrong about it?
Samantha: Well Tom is a very private person and er I wouldn't like to share stuff with other people that he's sent specifically to me without having asked his permission to do so
Fieldworker: Okay. So you need the right to t- t- to be able to share it you feel And er you wouldn't just have that right automatically to share it
Samantha: No
Fieldworker: Okay. Does that go for other content that you receive from other people on social media?
Samantha: Yeah, I don't- I don't share stuff like that because as I said it's something that's been sent specifically to me and I wouldn't share it without asking somebody if they were okay with that

Here we see how data that has been shared with you by other people is not necessarily oriented to in the same way as your own data. In particular there are chains of accountability such that the onward sharing of data is organized around one's right to share it in some way. These may be presumptive or they may be literally subject to having been given the right to share it somehow. So, in the case of Simon watching Maud using Facebook she was largely oriented to a presumptive right to let him look at the content and he himself was oriented to a presumptive right to see that content, even though much of what he was seeing had been shared with Maud by other parties. However, for Samantha she does not orient to a similar right to share things that have been specifically shared with her by her brother. Indeed, in further discussion it became clear that, whilst she would happily report to her parents and siblings that she had been in communication with Tom via social media, she was not disposed to then evidence this through specifically showing them the content of the interchange.

5.1.5 Keeping things from view

Of course, the very visibility of things in shared environments can also result in practices that are designed to *offset* the possibility of incidental sharing. Particular articulations of this point in the digital realm have already been made by a number of researchers. Hawkey and Inkpen [36], for instance, looked at people's privacy concerns in the context of witnessed online browsing and what they termed 'incidental eavesdropping'. This was deemed to be "information that can be gleaned from casually viewing the screen of a user or overhearing a conversation". Both they and Kaasten et al [40] have also extended this consideration to what traces people may leave behind regarding their activities for subsequent users through artefacts such as browser histories and saved thumbnails. In order to avoid any risk of exposure they suggested that people adapted their browsing activities according to different settings, different devices, and the kinds of people they had around them. Dourish et al [23] when looking at how people went about managing digital privacy in the workplace found that people were employing "subtle practices to achieve privacy and security goals, such as positioning a computer screen such that visitors in an office could not see it, or stacking papers according to a secret rationale." In another related study Klasnja et al [44] focused upon how people tried to preserve their privacy when using devices in public places and observed that they were using strategies such as "tilting or dimming the screen, or finding a seat against the wall".

In the studies being drawn upon here there was a range of similar phenomena, with various kinds of concerns about visibility being articulated. The following vignette is interesting because it relates

the handling of digital content to the handling of other physical components of the home environment. The interlocutor here is a 63 year-old reflexologist who runs her practice from home:

Fieldworker: … your clients are always coming to the house. Are there things that you do to manage what they can see at all?
Christine: Yes, I mean I'm big on er making sure that the whole house isn't open to their view. So I'm forever closing doors and shutting things off. I make sure everything is clear that I consider sensitive which is why, when I used to be in that smaller room particularly I did not want my laptop there, open while I was about to start a treatment. So that- er, that's when it's-
Fieldworker: So that window into your digital world actually you th- you consider ones you prefer to have closed to clients as well?
Christine: Closed off. Absolutely. Absolutely, and e- obviously I have to make sure that I don't leave information about previous clients lying around for now clients to see. So I have to-
Fieldworker: So it's both professional and personal reasons kind of wrapped in together?
Christine: Well absolutely because you know, I could be sued if people felt it was a breach of data protection so er I- I::'m- I have to be aware of that. So I don't have anything lying around tha- that in any way gives any window into anything And I don't keep my purse or my phone in the room with me either. That's always elsewhere
Fieldworker: Okay. And with regard to the network, I mean if- I mean I- I don't know that you're that busy that it would be a circumstance but if you had one- clients backing up where one was waiting for another one to go, would you give them access to the network?
Christine: No. Absolutely not. No, no. I wouldn't even give them access to the television unless Brian's [her husband] in the room watching it!

In this case we see someone operating a fairly blanket policy that is designed to minimize the risk of any kind of incidental sharing of personal information of any kind – digital or physical – with visitors to the house with whom the relationship is confined to business. She provides an account directed towards breaches of data protection, but in fact she is also closing doors and generally constraining their movements so that it is not just data relating to other clients but as much as possible of her own personal life she is keeping from view. However, when it comes to other members of the same household we begin to see much more nuanced kinds of practices coming into play. Here Evelyn, the 21 year-old student living at home, who expressed such concern about not sharing anything on Tumblr with others around her unless she chose to do so and could retain control, explains how she is actually nonetheless quite happy to browse Tumblr with other people around her:

> Erm well being on a phone it's a smaller screen so there is less oversight and I tend to keep it quite close to me anyway, erm So I'm fine with browsing Tumblr when erm when like I'm sitting on a chair downstairs and there are people walking about or when we're about to watch something

The overt point here is that she can manage keeping things from view quite adequately by simply relying upon the size of the screen and the way she holds it in relation to her body. More to the point here is the fact that doing this is not, in itself, treated as being accountable by others around her. So there is a mutual orientation to the content she is handling not being for general consumption. Indeed, it would be far more accountable for someone else in the family to sit beside her or try to lean over her shoulder to see what she was up to. So there is a mutually understood right to keep things from view that people routinely trade upon such that what might at first sight be viewed as 'guarded' behaviour is nothing of the sort but rather an everyday method for making manifest the status of particular kinds of personal data as 'not to be shared'.

There are a couple of things to point out that arise from the contrasting examples above. The first of these is the articulation of quite generic, blanket policies regarding whole classes of people such as 'strangers', 'visitors', 'clients', etc. when it comes to what might or might not be shared with members of such a class. This is not about what you do when Joanne, who is a friend of one of your friends and working in a bank comes to have her treatment on a Friday evening, or Aunt Sally who you've agreed to do a session for during an afternoon visit. When one inquires into the particulars of just what is done with this person or that one encounters a world of variation and contingency where specific differences of practice are accounted for in ways that make them acceptable variants of the overarching policy such that the policy can remain intact. So Joanne can sit in the living room and watch telly while she's waiting because I've known her for years and it wouldn't seem right putting her in the waiting room like everyone else. And I don't need to worry

so much about tidying everything out of the way and out of sight for Aunt Sally because she's my aunt and not even a proper client.

The other thing is that, when it is people who are known and who are specifically identifiable and with whom you hold a specific relationship of some kind, there are equally specific bodies of practice that come into play. So Evelyn can sit and browse Tumblr in a specific fashion in the living room and trust that she does not need to share any of it with those around her, even though they are the people with whom she holds the most intimate of relationships. And all of this turns upon the manifest way in which she handles the technology and the fact that everyone around her *accepts* that she should handle it that way. Hawkey and Inkpen [36] do note that, in the context of their usual browsing habits, many people are actually more uneasy about family members seeing their activity than co-workers. However, they do not seek to unpack the particularities of this blanket policy and see how it might be operable as an actual body of practice, turning instead to the formulation of 'four dimensions that directly impact the privacy comfort level [of people] in a given situation'. That is, they seek to make general formulations of policy yet more abstract and generic. But what is interesting here is the evident tension between what Evelyn has to say about her practice and the observation of the interactions around health data and Facebook we saw in the case of Maud and Simon earlier on, where personal use of social media was notably *not* being kept from the view of another intimate. So, there are intimates and there are intimates and they are not all of a piece. Instead, quite specific rights and obligations pertain to each specific relationship within a household and it is at this level that the *practical* politics of sharing comes into play, which is a politics of assumed rights that is almost never overtly articulated outside of a breach (such as someone pausing to look over Evelyn's shoulder or Maud actively waiting to look at Facebook until Simon has gone to bed).

5.1.6 Accountably appropriate sharing practices

The implications of the preceding materials are that a great deal of personal data is *already* being shared on a routine basis within the confines of cohort relationships that are already well-understood and where expectable patterns of accountability for what is or is not revealed and what is or is not done with information are oriented to in ways that are frequently very similar to other ways of sharing information. What is shared may be in some ways distinct in terms of detail and representation, but it is not as if cyclists were not telling one another about their state of health before the use of fitbits or husbands and wives not telling one another about their weight before the invention of Withings scales. And husbands were routinely listening in on telephone conversations between their wives and family members or friends before the invention of Facebook.

What should be stressed here is that the practical politics is to be found in just how specific instances of sharing personal data are organised. It is visible in the haecceity – the just whens and just wheres - of the sharing. It is present in just how the possible occasioning of sharing is picked up or set aside. And it is present in just who is oriented to as a potential recipient of the data. Some have rights to ask for it. Some have rights to expect it to be produced as a matter of course. And some could only ever expect to be given access to it upon the production of a specifically appropriate account. We have also seen how the politics of the sharing is organised around how the surrounding accounts for the data are themselves constructed according to different recipients and different circumstances. And we have seen how it is present in the very reasoning attached to what should or should not be shared. All of this adds up to a body of accountably appropriate sharing practices that cannot be divorced from, indeed are reflexively constitutive of, the circumstances in which they are used.

5.1.6 What is visible in the breach?

So far we have examined a range of ways in which people are already oriented to the management of personal data with regard to what is shared with other people around them. Now the thing with personal *data* is that it presents a number of challenges for the operation of these ordinary ways of

managing what is shared. For a start its recognisability as useable personal data is not always evident, prior to it having been gathered and displayed in some way. Another thing is that assumptions regarding who may get access to personal information are not always adequate for the handling of personal data and its articulation through digital devices. Indeed, recognition that something has been revealed may only come latterly after sharing has already taken place. These are all issues we shall return to in the conclusion because they carry implications for how designers might need to be thinking about the handling of personal data. Over the course of the ethnographic work a range of breaches of ordinary expectations were uncovered regarding the sharing of information that have turned upon the fact that the vehicles for sharing have been digital devices drawing upon personal data. It is worth briefly examining some of these breaches because they are instructive, *alla* Garfinkel [29], for the assumptions made about the ordinary orderliness of the world they reveal.

5.1.8 The recipients of shared data

A particular issue that has already been partially reported elsewhere [75] is the potential for new technology to surface information about one another's activities that would ordinarily be expected to remain out of view. Or, at least, for the circumstances to not arise where one might be obliged to account for it, and for others to be put in a position where they have little choice but to request such an account.

As we have already commented, the cohort that are most likely to call people to account for such activity are those with whom more intimate relationships hold, e.g. parents, siblings, partners, etc. In the following excerpt the issue relates to what is being made visible about a teenage girl's late-night internet activity to her parents. The fieldworker and the participant, Coralie, are looking at some periods of exceptional activity in a data visualization tool. They are both sat at a table in the living room and the participant's parents are sat on a nearby sofa watching television while they talk:

Fieldworker: Look at the time. This is after 3 in the morning

(Coralie glances over towards her parents)

(Fieldworker talking her through the pattern)

Fieldworker: It's completely different to every other day.
Coralie: When was it?
Fieldworker: This is late at night – from a Saturday to a Sunday. If you look you can see you were using it through to late into the morning

(Coralie casting more nervous glances at her parents)

It's a familiar trope in households with teenage children that they take themselves off to their bedrooms and their parents never know what they're up to. For younger teenagers this may become centred around a concern they are looking at porn, or watching violent videos, or chatting online with dubious strangers, etc. At the same time, for teenagers themselves the closed bedroom door provides a vehicle whereby they can themselves hold their parents to account for any breach of that barrier and inspection of their activities. This may or may not be contested but the door remains as a visibility management device. Other discussions with Coralie had revealed that she almost exclusively used her laptop and went online in her bedroom. Use of the laptop in the living room was rare and the use of it with the fieldworker at the living room table was a notable departure from her routine, such that it was remarkable to her parents as well and only readily accountable because of the interaction taking place with a 'guest'. What we see in the example above, then, is the closed door and its operational efficacy being breached by the surfacing within earshot of her parents of activities that would normally be happening behind the bedroom door, hence her evident discomfort.

As we saw previously with a husband and wife sharing heath data, many instances of sharing personal data are part-and-parcel of the realization of existing routine practices. However, what was also seen on a number of occasions was personal data and its visualization resulting in the exposure of activities that people would normally take for granted would remain invisible.

Here is another example that was captured during the sensor data study. In this case a husband and wife are working with a researcher through a visualization of motion and humidity data for their bathroom:

Susannah: So what are we saying, we're saying the 5th? That was Mary being off and the 6th was you being at home. Oooh, what did you do?
Frank: I didn't do anything
Susannah: You did at 12 o'clock, look at that
Frank: Where? Nothing
Susannah: No, here
Frank: I could have been up late cos I've had this headache thing… I've been a bit poorly, oh give me sympathy. So, that's probably me getting up late isn't it, having a late shower. It's high for a long time…I don't remember having that long a shower.
Susannah: Yeah but you could have had a shower and then you could have had a shave.

It is, of course, the case that people's bathroom practices can be subject to comment as a feature of ordinary life in all sorts of ways. Toothbrushes may be left on the side or the toothpaste squeezed in the 'wrong' way. Towels may be left in a heap on the floor. All of the hot water may be used up. And so on. People can also specifically make their own bathroom practices visible as a vehicle for calling others to account. For instance, calling out to say they are about to have a shower so that other people don't turn on taps and make the shower run suddenly hot or cold; saying where they like to keep their flannel because someone keeps moving it; calling out their weight from the bathroom because they've just stood on the scales and it's gone down; and so on. In all these kinds of cases you normally understand somehow what will be available and manage your affairs accordingly. The presence of this new window into what you do stands outside ordinary everyday reasoning, especially with regard to the expectability of the possibility of needing to provide an account and the knowledge of how your activities might be routinely made available. And this has the scope to cause serious trouble.

Here, in the same family, we see sensors revealing data about their daughter, Sally's toilet practices that go to the heart of the accountability issue:

Susannah: So, I'm aware that there's evidence that Sally's gone for a wee when she's spent most of her life trying to, at the moment, defining her space and David [their son] is defining his space. So now there's evidence, so now I can see into these spaces, so there's a sense of invasion. I can now look and find out who went for a wee when and where they went.

The problem with surfacing data of this nature is that the accountability cuts strongly both ways: those in receipt of the data are as accountable for taking an interest in it as are the people who are generating the data and unwittingly sharing it in the first place. In shared environments there are many things that people have, over unknown stretches of time, developed ways of keeping unremarkable so that as far as possible people are not obliged to have to continually account for 'uncomfortable truths', or to have to account for how you handle the management of those uncomfortable truths if you become privy to them in some way. But we are moving towards a world where we may need to find new methods for rendering uncomfortable truths unremarkable, and it would be wrong for designers to be complacent about how such uncomfortable truths might get surfaced in the first place.

5.1.9 How data may get used

A further matter that cropped up over the course of the studies being discussed here that is tightly related to the preceding set of issues is the way in which, once personal data is made available to others around you, it may then be used by those other parties. Once again the problem here is bound up with the fact that people have not yet fully organized the management of their personal data such that inadvertent and awkward revelations can be foreseen and avoided before they ever take place.

In this next example Florence and her mother are visiting a boulangerie. Florence has been helping her mother build a website for the novelty cakes she makes and has been taking photos of the cakes with her phone. The fact that her mother knows this results in an uncomfortable situation for Florence:

Fieldworker: Do you ever give i- er access to your phone to anybody else at all?

Florence: Er:m, I mean I do, like, when I'm showing photos or things online to people mostly, but er

Fieldworker: In what way do you mean you give them access? Do you kind of hold your phone and show it to them?

Florence: Yeah.

Fieldworker: But you don't let them physically take the-

Florence: No, no. That was er actually something quite uncomfortable for me that happened the other day when erm- because you know er I went to the cake shop with Mum and she started talking about one of the cakes she'd made and then she asked me if I had any photos on my phone, and er I did so I just held it up to show at first but then Mum took the phone from me and passed it to the- to the man so that he could flick through the photos and look and I did not like that at all

A core part of the trouble here revolves around the fact that there is a mismatch of understanding about what the work of showing might amount to. Her mother knows the photos are there and is only oriented to being able to show those photos to support the ongoing interaction. Florence, however, is oriented to the fact that these are just some of the photos in her undifferentiated photo library. For her it is the photo library that is potentially being put on display. This underscores the relative crudity of digital resources and demonstrates the fact that personal data may be bundled up in ways that do not reflect adequately people's ordinary reasoning about content and what may be done with it, and this is something that designers would again do well to reflect upon.

We will shortly be looking at the sharing of personal data online. However, there are some ways in which data shared online may nonetheless lead to troubles in co-present interaction. Here we see an example of how content shared on Facebook may be exposed in awkward ways that are challenging to deal with:

Sylvie: I tried for a while having people graded by their friendship status. So I'd have like real true friends, and then I had my work friends, who would ask me to be their friend but I felt kind of like socially awkward saying no to on Facebook, so I had them as acquaintances. It got really confusing. You know, someone might graduate from being an acquaintance to an actual friend but they still work with you, and then they come into work and say "oh I saw that picture of you at the park, it was really cute" and everyone else goes "what picture? I didn't see that on Facebook." So, I've given up on that. It just got really hard.

Once again there is a mismatch of ordinary assumptions in play here. This revolves around an important issue: the practices people adopt to try and manage their personal data in the digital realm are not simply just there to be seen and oriented to by other people. These are not yet practices that just anyone would recognise and organise their interactions in respect of. In many cases they have not yet reached the point of becoming routine member's methods and cannot yet be taken for granted. It is not the case, of course, that people were not being embarrassed by awkward revelations before technology entered the scene. However, the interesting thing about examples such as the one above is that the source of trouble is not so much the content itself as the lack of a developed intersubjective understanding of the practices people are using to manage their digital content. How might Sylvie's co-workers have known that she was adopting a practice of organising her Facebook friends in such a fine-grained fashion when this is not what just anyone does when they manage their friendship relations on Facebook? Thus the practices present here are part of a practical politics of sharing that has yet to adequately evolve, and a key sticking point in it all is the extent to which technology is a) supporting and b) making visible the practices people are trying to adopt to handle personal data.

5.2 Sharing personal data online

5.2.1 Managing how the data is shared

The materials above have focused on how personal data might be shared or not shared with other people who occupy the same environment. However, it is of course the case that an increasingly large variety of the digital activities people undertake are geared towards interaction with parties and organisations who are *not* co-present but rather accessed through networks online. These parties may, in principle, be anywhere and, unlike the local cohort, may be oriented to as both known members of various cohorts and as unknown or unknowable beyond what common-sense assumptions may be made about them and their interests. This has an important impact upon the

sharing of personal data because there is a vital interplay of rights and obligations and intersubjectively established accountabilities according to the specific nature of the relationship in play. And if there is no established relationship because a party is unknown or unknowable then the grounds of mutual accountability are hard to assess beyond the broadest of moral assumptions (e.g. 'no-one in their right mind would do that!').

One particular way this pans out is an exhibited concern with allowing data to be shared before you have had an opportunity to inspect the data and potentially repair it or at least premise the data with some kind of an account. Something that made this kind of interest manifest in the data collected during the studies was a worry people had about data being potentially made available 'live'. All of the following excerpts were articulated by participants in a study where the concept being explored was the collection of sensor-based data that could reveal information about your patterns of living and then sold through an online marketplace to external service providers.

Celine: I wouldn't agree to live, I would agree to an embargo for example, a month a week, two weeks, because you can deduce whether we are home or not from that data if it was live, you can deduce the actions of the people.

Connie: But it's different isn't it, live sharing, there's quite a different set of feelings that this could evoke… I think you could manipulate the data anyway by not using that room or not weighing yourself, or not very much, or only weighing yourself when you're feeling… or dieting on purpose in order to record it so that somebody else approves of you. So I think when you're sharing live you can't do anything about it so people naturally want approval from other people so I think that would influence you so I would I would feel less comfortable sharing live I think.

Andrew: Some of the data I'd be quite happy to share live. So, sharing live weight data with my GP would be fine. With my insurance company, though, it wouldn't, because it's the purpose, what they might use it for…

Note that in each of these cases there is an issue with live data because they feel it would be hard for them to control what other *reason-able recipients* might make of it: potential house-breakers; people from whom you might be seeking approval; or insurance companies. Here each of the parties is in some sense an unknown and generic member of those categories, so accountabilities are equally generic: what anyone might expect of house-breakers, potential approval-givers, or insurance assessors. In each of these cases there are still ways in which the interests of the parties being shared with are open to being reasoned about so there are commonsense assumptions about each of the categories in play. But sometimes it can also devolve to being just people in general as well:

Celine: I wouldn't be content to share it with anybody, except friends or people I know or who might have a reason to… why would you want to have it? Why would anybody want to have it?

Of course, much of the time online data *is* being shared with known cohorts where the understood grounds of relationships are in play. The following sections examine some of the ways the practical politics of sharing gets shaped around this.

5.2.2 Managing potential recipients

A great deal of the sharing of personal data online happens now via various social media platforms. This was visible across the studies and there are several mechanisms people may use to control just who the recipients of that data might be.

One such mechanism is through actively tailoring just who is a member of which cohort that you share with.

Fieldworker: And the Facebook friends are? `Erm who?
Chloe: People I know… That's basically most of my family, er and my friends and a few people that I know from school who asked me as a friend and so I just accepted coz I know them. But if it's anybody I don't know I won't accept
Fieldworker: And, and do they overlap with your Twitter people? Do you have the same that you're er- as Facebook friends that you're following on Twitter or following you?

Chloe: No
Fieldworker: No connection between them at all?
Chloe: No, my social life has nothing to do with my Twitter life… Twitter life is internet life. And Facebook life is social life

Time and again in the studies there were examples of people taking great care over just who they follow and whom they encourage to follow them on social media platforms. This was particularly notable with regard to constraints being placed upon the opportunities for people they know in the real world to follow them. This shall be discussed further below in terms of avoiding real-world accountability. However, note here straight away that this management of cohorts amounts in online practice to management of sharing personal data because the information shared on such platforms only goes to the people who are following you. And it was clear that people actively reasoned about the mechanism in this way.

With this in mind some will even go so far as to adopt pseudonyms for distinct interactional environments[7]:

Melanie: Okay so Tumblr's more interesting because I have my:::: m::ain account where I'm *me*, I have my::; (.) *art* account where I'm me, but then I actually have a *joint* account on Tumblr with M [a friend] where we pose as our supervillain characters
Fieldworker: So what's the distinction between yo::u as you and you as your art account?
Melanie: Er:::m coz me I can just post whatever I'd- I'd have to say Tumblr is probably the place where I'm the most (.) personal, where I er, *will* share stories that I wouldn't share with just anyone
Fieldworker: Okay
Melanie: Er:::::m But on my art account I- I'm still::: *me* but er::m (.) bu::::t I try and keep it a bit more professional … I have two main kind of online pseudo- pseudo- (.) pseudonyms which are Melanie Tea [anonymised], as in Tea the drink and er:::m, and O T O [anonymised], and on some places I'm *both*, and some places I'm one or the other

Whilst this does not amount to the management of personal data per se, it was evident in the studies that an important part of the reasoning attached to the adoption of pseudonyms is the avoidance of being discoverable online by people who know you. People actively seek out others they know on social media platforms and will not hesitate to make friend or follower requests if they recognise someone. The easiest way to steer this off is to make yourself unrecognizable. In this way there is no need to potentially have to account for why you have turned down or ignored a friend or follower request to people to whom you *are* routinely accountable in other ways. But it also carries the advantage that there will be less chance of sharing personal data with people you would not ordinarily wish to share it with. And it is a testament to the current crudity of such tools that people have to adopt such blunt instruments to manage their accountability to others and their sharing of personal information.

An alternative method is to actively select just whom content will be shared with on a case-by-case basis. Here is an example from a study of digital privacy management where a couple being interviewed together were discussing how videos of their children were shared with other people:

Fieldworker: Who has access to the videos on Vimeo?
Kit: It's just family, isn't it?
Tim: Yeah, family.
Kit: They tend to be on holiday, it's not like there's anything - if the kids were, say, running around in the nude on the beach, then I wouldn't like it.
Tim: Yeah.
Kit: But I don't think there's anything like that really.

Here the problem is perhaps more acute in that the personal data in question involves family members who may or may not wish to have their activities open to inspection by other people. So at least a part of the reasoning here relates to issues that were already outlined above regarding the sharing of third party data.

[7] There is, of course, a whole literature regarding the management of online 'identity' that relates to this, e.g. [80] but we have not the space to tackle this topic directly here.

5.2.3 Specifically targeting recipients

The above example might be seen to be a case of specifically targeting certain recipients, and in a certain sense it is. However, sharing personal data can be even more specifically targeted in online interaction in various ways. In the following example from the study of the management of digital privacy one of the participants recounts how Facebook Messenger was used by another family member to interact with her about a topic she clearly didn't want to share with just anyone:

> My niece, indeed all the younger members of my family, have created a group on Facebook called 'Dubois family'… And in fact two or three times I was contacted by Messenger by my nephew or my niece… about something private that didn't concern the rest of the family. And because they didn't know my email address they contacted me that way instead… about private stuff, someone who had a miscarriage, another where they wanted an address, things like that. So it's true that whilst I don't use that so much, I do use the direct messaging on Facebook. It was a thing I didn't really use before but I've been using it now for a couple of months … It's private. I think for the other person as well it's very private because otherwise they would have sent it to the whole group. She also phoned me, but younger people nowadays of twenty, twenty five, they find it easier to use Facebook, and so she found it was a good way of talking to me directly.

There are some interesting things here that are worth teasing out a little. Now clearly there are a number of vehicles for talking to someone on a private channel when you're wanting to discuss sensitive matters such as having a miscarriage. You could do it by email, or text message, use Skype, maybe even, as Denise mentions above, make a phone call. But there's this thing here of them having made a family group and doing their family interactions in that fashion. A comparable example to think of here might be family homes and where people have conversations within them. And then one might think about private conversations between, say mothers and daughters. Now, if the daughter has a trouble to communicate with her mother about but doesn't want the rest of the family to know, she might ask her mother to come into her bedroom, or go visit her mother in her's, or she might wait until just she and her mother are alone in the kitchen or wherever to broach the topic. What would be much stranger would be for her to send her mother a note, or a text message, or an email, or even a direct message on Facebook, even though she probably could. Denise puts the choice of Messenger down to her niece's age, but it also needs to be recognised here that there is an existing place where family conversations are happening and her niece has found a resource within that space for having a private conversation. There is no special work to be done or accounting for the choice of channel to be concerned about because they are already communicating via Facebook. At the same time, because it is in the nature of direct messaging that it be one to one, the niece can hold Denise accountable for what she may then do with the information, and the presence of this accountability is also visible to Denise. So what we see here is people finding within an online resource a practical solution to the sharing of highly personal data and, most especially, accomplishing that through a resource that is ready-to-hand *for both parties* rather than having to go out and invent some other one.

5.2.4 Avoiding real world accountability

It was mentioned above that an important feature of the practical politics of sharing data online is the way in which people actively manage the cohorts that will be able to see their data through friend and follower relationships on social media platforms. Time and again the reasoning attached to this body of practice was articulated in terms of how people could use this mechanism to avoid real world accountability for the things they were sharing. Here are just a few examples:

> **Fieldworker**: And what kinds of people are following you [on Tumblr]?
> **Melanie**: Erm Very few people who know me in real life. Very, very few. There's literally only Lionel and Tom [her brothers] I think who actually know me in real life. That's probably why my- I'm more comfortable being more personal there coz there's less people I actually know personally
>
> --
>
> **Paul**: I've got Facebook and I've got Twitter. I have a network of friends on Facebook that includes my family, some colleagues, things like that. On Twitter, even though I use my

proper name, I don't follow anybody that I know personally. I quite explicitly avoid connections with especially work colleagues on Twitter. I don't follow any of them and I don't want that link to be made, because I want to be able to behave in a different way on Twitter.

--

Simon: Most people I follow on Twitter, they don't know me and I don't know them. So I'm free on Twitter. [Laughs] I'm free there, I do what I want.

Something to take note of here is that the platform where people were choosing to share data that they would not want to be held accountable for in the real world differs from person to person. In the above examples, one person is speaking of Tumblr, two others of Twitter, but there are other examples where it is Facebook and even where it is a different account on the same social media platform. The point to emphasize here, though, is that the orientation is not directed towards a specific platform but rather towards a *practice* whereby real-world accountability can be set aside. It's important to understand here that the concern is not with dispensing with all accountability entirely, but rather with managing just who you might be accountable to and in what way.

5.2.5 Managing what is visible

When the sharing of personal data in the context of co-present interaction was discussed, one of the primary concerns people exhibited related to what was being made visible to others around them and how to manage that visibility in various ways. Part of this was focused upon what was being overtly shared with others or not. However, another aspect of it was focused upon trying to limit the scope for data to be shared incidentally, unwittingly, or even unknowingly with others who might happen to occupy the same space as you. The risk of incidental data being shared about you online may seem to be particularly related to various kinds of security breaches and hacks, or big data style harvesting of your interactions by large organisations such as operators of social media platforms or governments. It has already been discussed elsewhere [21] that most people tend to orient to this as something more or less unavoidable and to continue regardless. In the same place it was also noted that some people will go to great lengths to try and minimize the scope for this through a variety of technical strategies. However, it is also the case that the concerns people have about what they may be making available incidentally can be reasoned about at a much more parochial everyday level and with regard to people who one already knows. And this can lead to some quite nuanced approaches to managing what is therefore made visible. The following is an extract from a discussion with a participant in a study geared towards investigating people's online practices to inform the development of a 'context-aware' media delivery platform:

Charlene: I use the phone more than- the computer because that can give the impression to other people that I'm not at home… Whilst when I'm on the computer it's obvious that- … I prefer to make my location more obscure (laughing) … Because for example if I want to end a conversation with someone I can say 'Sorry, I'm about to take the metro, sorry'. … Or 'I've got a meeting'

In this example Charlene is actively managing the ways in which her practices may make visible incidentally her current location. At root there's a quite simple set of assumptions going on here. If people you know are interacting with you via a desktop machine then the chances are you also know where that desktop machine is, most often in that person's home. That means you can work with an expectation of them being at home to organise your interaction with them, say in terms of their likely availability. If they are interacting with you via a laptop and you happen to know that, then the options for being elsewhere are greater, but most people still use their laptops in a more restricted and knowable group of settings, so you are still able to make assumptions on the basis of that. However, if people are interacting with you via a mobile phone and they make it visible that this is the case, then they could in principle be anywhere where there's a signal, so it's hard to make assumptions about what they might or might not be doing in relation to where they may currently be. What the above example exposes neatly is that this reasoning has itself become a sociological object, a thing that can be reasoned about in its own right and managed and worked with to a variety of ends. In particular we can see here how commonsense assumptions about what people do with their devices provide in their own right a resource for thereby managing what might be made available incidentally to others.

5.2.6 Choosing whether to share data at all

In the preceding section reference was made to a commonplace assumption that there are organisations 'out there', so to speak, who will have access to one's personal data regardless. Whilst there is a background acceptance of this in place[8] when many online exchanges take place, it also informs a broad and generic 'policy' that people often articulate regarding choices they make as to whether to reveal data at all:

> **Christine**: if it was something tha- that I considered to be that sensitive, although there was a hideous picture, but i- if- if it was something that I considered to be that sensitive I wouldn't do i- I wouldn't use it
>
> --
>
> **Carrie**: If I'm not happy to share it then it doesn't go anywhere.
>
> --
>
> **Alice**: I wouldn't put anything on that I wasn't happy for anybody to see. Managing real private stuff is – stuff shouldn't exist, that's the level of it. It doesn't get written down. It doesn't get put in a photo. It doesn't exist. Definitely do not put online.

The description here of this reasoning amounting to a generic policy is important. Whilst risk of exposure and sensitivity of data stands as a ready account for not sharing something, it is also just as commonplace for people to share things online that they subsequently have cause to regret. Indeed, the literature is replete with examples of postings on social media that have escaped the control of their authors and resulted in embarrassment (see, for instance, [41][47][59][60][69][72][78][79]). As has been recurrently pointed out in this paper, the sharing of personal data is something that is actively occasioned and there is a calculus of accountability in play that informs what is or isn't shared on any occasion. Even at a gross level people are not sharing personal data with abstract classes of others but rather quite specific others about whom certain categorical aspects may be presumed (e.g. insurance people will raise your premiums if they find out you have a life-threatening disease). Thus, whilst people will articulate generic polices in response to questions they understand to be asking for what they generally do, when it comes to deciding whether something will actually be shared or not, the decision turns upon the specific occasion and what should be practically and accountably done *now*. And what is done now is not always what one would express to be the general policy. Instead, if questioned on the matter people will find ways of making the specific instance an allowable exception or somehow still honouring the policy in principle if not in practice. Inevitably this leads to trouble. The difficulty is that the nuanced reasoning people adopt about how the practical politics of sharing should play out, based upon their ordinary everyday understandings about how sharing should take place, is not always commensurate with the organisation and operation of digital systems, which do not adhere to the same principles of situated reasoning. More than this, it is hard to see how they could.

5.2.7 Sharing online versus sharing in person: differences and similarities

In the examination of the practical politics of sharing with regard to the sharing of personal data in co-present interaction it was noted that a great deal of personal data is already being shared on a routine basis within the grounds of established relationships with established patterns of accountability that are not far-removed from other kinds of routine information sharing practices. It was also stressed that the practical politics is to be found in the haecceity - the occasioned and situated grounds – of the sharing. On top of this the presence of specific rights and expectations were noted that are made manifest in just how the sharing is accomplished according to the recipients

[8] This is itself an important point because, for the larger part, it is clear that people do not sit and concern themselves with this afresh each time they share personal data online. Rather, actively reasoning about whether something might be made visible to third parties is an occasioned matter. That is, to take an extreme example, members of extremist organisations might take pause before sharing something that would risk making this visible to government, police or military authorities. As we also go onto point out in this section, however, it is notable how often the background expectation remains even in such extreme circumstances, and there are plenty of examples of people being caught out in just this fashion.

of what is shared. What we have seen in the sharing of personal data in non co-present circumstances, online, is something broadly similar. The sharing is once again occasioned and recipient-designed. People are once again oriented to what is or isn't made visible and seek to manage that accordingly, including sophisticated reasoning about what may be shared incidentally.

What is different in online sharing is the relatively crude tools available for managing visibility, just who the information will be shared with, and what kinds of accounts can be shaped within and around the content of the data being shared.

Something that underscores the *consistency* of reasoning across the sharing of personal data in co-present interaction and online is the extent to which concerns that are surfaced reflect the same kinds of considerations: Who is going to see the data? And, How is the data going to be used?

5.2.8 The recipients of shared data

As was noted above, an important difference between sharing personal data online and sharing it in co-present interaction is that the mechanisms available for exercising subtlety in how the sharing might be shaped to specific recipients are limited in online interaction. We've already seen how online sharing can produce unwanted accountability in co-present interaction with regard to the sharing of photographs on Facebook. However, the concern can extend beyond this and breaches reveal the extent to which cohort management through friend and follower relationships is a blunt instrument at best.

In the following example Michel expresses his frustration with the limited resources he has available to him for controlling what kinds of things get shared with whom on Facebook:

Michel:	One of the reasons why Carrie is not so sensitive about posting family photos on Facebook is because pretty well the only network who get to see that are family and friends. Whereas with me, the network who can actually see that includes work colleagues, some of whom I don't even know very well even. I mean, we've had photos of me in fancy dress for instance on Facebook and it's become clear that other people have had access to those things!
Fieldworker:	So it's other people's stuff that you're in and they've put up?
Michel:	It's never stuff that I share myself, no, 'cause I don't do that kind of stuff.
Carrie:	I do, of fancy dress (laughs). Have you seen that one (Carrie holds up her iPad to Paul, and then turns it to show the fieldworker).
Fieldworker:	(Laughs at photo of them both in fancy dress).
Michel:	(Laughs).
Carrie:	It's stuff like that he doesn't want me to put on.
Michel:	This is the problem for me. I can control it all I like myself, but I have no control over what other people do.

In some respects this reflects the example where sharing via Facebook caused trouble with how to organise relationships with co-workers. Here too there is an issue with how to manage distinctions between people who are apparently members of the same cohort, such as work colleagues, but with whom there are in fact gradations of rights, obligations and accountabilities that, in co-present interaction are managed eternally on a case by case basis. Indeed, the original example cited from Sacks is handling exactly this order of problem. With the ordering systems available on social media platforms people are pushed to what amount to generic sharing mechanisms which assume that all people in the same bucket are essentially the same when, in fact, everyone is potentially unique depending on just what is being shared in this particular instance.

However, this example also exposes more than this because, when people who have relationships in the real world are also friends and followers on social media platforms, there are all sorts of ways in which what is shared by one may become visible across a shared cohort, even though the reasoning each would apply to the specific data being shared may differ according to a wide range of possible rationales. This presents a fundamental issue. In online sharing like this people are not just pushed to generic solutions for sharing particular items of personal data themselves. They are also obliged to apply in advance and as a matter of course generic *policies* for the sharing of data. As has been previously discussed elsewhere [17], in ordinary everyday reasoning generic policies are typically used as either post hoc rationales around which particular accounts may be shaped for actions undertaken, or as blanket articulations of a point of view. They are not typically turned to and used to shape in advance specific instances of interaction. Indeed, it would be laborious to say

the least if every interaction we undertook required prior consideration in these terms. Instead, in practice the just whats and just hows of any matter are always related to the specific case in hand. When we are engaged in *co-present* interaction we manage the boundaries of what is visible and just how what is visible is articulated through a range of mundane practices that revolve around just how things are said, just who they are said to, just when they are said, just where they are said, and so on. Digital systems do not currently provide us with the same kinds of fine-grained mechanisms for accomplishing this. To do it presently would mean that for everything shared on social media we would have to take pause and reason about the current cohort we are sharing with and reason about how we might either need to change the cohort on this occasion or modify the content so that it is naturally and appropriately accountable to all potential recipients. That is clearly not what happens and so people live instead with the consequences and have to manage the breaches as they occur. What is breached, it turns out, is the practical, local politics of sharing, even if the generic politics that we might formulate in the abstract is apparently untouched.

5.2.9 How data may get used

Another important difference with the sharing of personal data online relates to the extent to which people may exercise control over how the data is then used through established patterns of accountability. In the studies it was found that people often articulate worries about how much they can control what is done with their data as a general concern. However, it is instances where they are confronted with its actual use that cause the most consternation. In the following example Sara expresses worries about the fact that recent advertising she has seen on Facebook would suggest that it has recognised she is Jewish:

> There's one thing that worried me though. Do you remember that time – my family's Jewish, and my uncle sometimes posts things, just once or twice, about searching for family in the Ukraine and stuff, and I was starting to find a shop selling everything Jewish coming up advertising on my page. So they've obviously made a connection that somewhere in the family there is somebody Jewish, and they've advertised that to me so that means obviously that it's visible to somebody. It makes you very aware that people are watching what you're doing. It's like I was explaining to Hannah [her teenage daughter] the other day. She was getting ads for pregnancy tests and she says, why am I getting this stuff. I said it's targeted because you're a teenage girl. And she said, but I've never gone on any site like that, I've never looked at anything. I said it doesn't matter, they can tell by the type of sites that you do go on to – they can put you within an age group and sex group and so you're targeted. She really doesn't understand that even so. She says I go on gaming sites, I could be a boy. Yeah, you could, but even so the indications that you give are a flag to somebody.

There are two matters to be considered here. One concern she expresses is that the data has been used. However, the other relates to the fact that she does not understand how this data has been acquired because it's not data she believes she has personally shared. From the account we can see that this was the case for her daughter as well. A key issue to reflect upon here in that case is: What counts as sharing in the digital domain? The cited example makes it clear that for most people at present the system is opaque. This goes beyond what we have just been saying about the crudity of tools available for managing relationships online and the way they pre-configure sharing on a generic basis. What we can now see is that it is not just that digital systems oblige generic rather than situated reasoning to exercise management, thereby derailing the case by case shaping which is at the core of the practical politics of sharing. It is also that digital systems do not necessarily count as sharing what *people* would recognise as a practice of sharing and do not make themselves evidently accountable for the handling of what is shared in the same way. This, of course, goes to the core of understanding what counts as data, and, more than this even, what may be done with personal data by digital systems as opposed to what may be done with it by other people where certain aspects of everyday intersubjective reasoning may be brought to bear.

6. ENABLING THE PRACTICAL POLITICS OF SHARING

This paper has used a range of studies of the everyday sharing of personal data to examine what the *practical politics of sharing* personal data looks like under two contrasting conditions: the sharing of data in co-present interaction; and the sharing of data in distributed interaction, i.e., online. Along the way we have seen how there is a variety of existing practices for handling the sharing of personal data, many of them very similar to pre-existing practices for sharing personal information, or at least grounded in a similar body of reasoning. At the grossest level this may be seen to cut across two broad dimensions: 1) What is made available to whom and when; and 2) How what is shared is to be understood (and what may therefore be done with it).

With regard to the first of these, in circumstances where personal data is being shared in co-present interaction people do things like managing access itself through physical control of their devices, managing just who the recipients are and managing what is visible to others both as a matter of routine and as a matter of keeping stuff from view. In online interaction people may manage when their data is made available, they may manage who gets sight of it through mechanisms such as friend and follower relationships, they may exploit commonsense understandings of how technology is used to limit what can be made of their activities, and they may, of course, just choose not to share things at all.

With regard to the second dimension, in co-present interaction people actively manage the exact situation in which data is shared and they craft how others may orient to it through its juxtaposition with verbal accounts. We also saw that people are highly attentive to their own rights with regard to how they may then make use of personal data that others have shared with them. In online interaction we saw how people make use of certain features of the systems they use to render other people accountable for what is then done with their data, typically by targeting or filtering recipients in various ways.

Now the point we reached in the previous section would seem to indicate that there are serious issues confronting the design of digital systems with regard to how they handle the sharing of personal data. However, as the outline just presented should make clear, a great deal of this paper has actually been concerned with articulating how people are already sharing personal data, and the methods they are using to accomplish that. So it is evidently not the case that digital systems are entirely *obstructive* to the sharing of personal data. Indeed, this would be a hard claim to make in the face of the countless millions of successful digitally-mediated interactions that happen every day.

The fact that people somehow accomplish the sharing of personal data in the digital world, and that they are somehow evolving a body of practice whereby they can accomplish sharing as ongoing matter, is not reason to be complacent or to assume that digital systems are already good enough and that it is simply a matter of time before people come up to speed. For all that people evidently make do with what the digital provides them, it is evident too that the digital world is routinely encountered as a 'troublesome' place that *breaches the calculus of accountability governing the practical politics of sharing*.

As this study makes clear, in the real world, in face to face encounters, data sharing is 'recipient designed' – i.e., crafted in specific places, at specific times, in specific ways, for specific people. Furthermore, the interactional design of moments of personal data sharing is necessarily an 'occasioned' (whether incidentally or purposefully) and a morally ordered matter that constrains the onward sharing of data. The rapid dispersal of data, and the potential for new technology to concomitantly render people accountable for matters that might ordinarily be expected to remain out of view, routinely enables the digital to breach the moral order, thereby disrupting the calculus of accountability governing the practical politics of sharing. Core to the disruption is that digital systems derail the case-by-case interactional crafting and shaping which is at the core of the practical politics of sharing, and instead oblige people to engage in generic rather than situated practices of action and reasoning to manage the sharing of personal data in the digital world.

Nonetheless, our study has shown something of how people routinely manage this disruption and bootstrap the breach. It taps into and allows us to witness elements of an evolving online calculus of accountability geared towards governing sharing in circumstances where parties to the occasion are *not* co-present and are potentially *unknown*. In such commonplace circumstances in the digital

world it is impossible for people to control what other recipients might make of their data, and even who the recipients are or might be. We thus see people taking great care over the management of cohorts, identities, and the visibility of the digital self to reduce the chance of sharing personal data with people they would not ordinarily wish to share it with.

Time and again the reasoning driving this evolving body of practice is articulated in our studies in terms of avoiding real world accountability for the things people share online. This is not, we note, a concern to dispense with accountability entirely, but rather to manage just who it is persons might be accountable to and in what ways. Thus, the evolving calculus governing data sharing in the digital world seeks to *constrain* the accountability of persons and their digitally-mediated interactions. This is a particular challenge in a world where what constitutes personal data is being reimagined on the fly by technological platforms.

Manifold elements of the digital footprint automatically harvested by digital systems further disrupt the moral order when they are eventually surfaced and become apparent. People are trying to handle this intrusion (the rise of ad blockers, for example, is pronounced), but more is needed and design should not then rest on its laurels and leave people to work around the troubles that accompany data sharing in the digital world. Rather, design should seek to support the calculus of accountability that provides for data sharing in the real world, and it should do so not as a matter of moral compunction but because it will gear the digital into the practical politics of sharing and thus *enable* rather than disrupt personal data sharing.

Key to this achievement is to recognise that there is more to the sharing of personal data than data. Clearly, it will be important to articulate what data is being shared, especially with respect to underlying and evolving technological platforms, and this is clearly starting to happen, e.g., through new data protection regulations and a growing interest in making algorithms accountable. However, it is equally important to transcend generic mechanisms and support the *haecceities* of data sharing to enable people to manage just where, just when, and just who gets access to their data and to determine just what of it gets used and just what it gets used for by whom, whether incidentally or purposefully, on a case-by-case basis in the ongoing course of digitally-mediated interaction.

In talking of the haecceities of data sharing we are not talking of enhanced privacy settings that provide a more extensive range of generic pre-specified polices, but of making a massively distributed environment of connected persons, things and black-boxed systems accountable to people and tractable *in the moment of sharing*. Thus design on this view needs to explore ways of providing support for the sharing of data that moves beyond gross pre-specification, as opposed to nuanced situated specificity. Providing more granularity, for instance by giving lots of sub-cohort options, does not fix the fundamental problem of pre-specification because people *do not know in advance* what every instance of sharing will look like. Concomitantly design needs to provide transparency to users regarding what their data looks like to the system and what 'politics' might be applied to it. Thus systems need to account for what constitutes data and what they assume they can do with the data, including what is intended to be achieved by the parties to sharing *in* situated instances *of* sharing.

The extent of these challenges should not be underestimated. As Harold Garfinkel reminds us, *"A society's members encounter and know the moral order as perceivedly normal courses of action – familiar scenes of everyday affairs, the world of daily life known in common with others and with others taken for granted"* [29: 35]. Digital systems today pervade everyday affairs, but do they really share this world of daily life known in common with others and gear in with perceivedly normal courses of action? To some extent, yes, but they ride roughshod over the practical politics of sharing at their own expense. Design may well benefit, then, by complementing a concern with privacy with a concern to build the calculus of accountability into an increasingly networked world.

ACKNOWLEDGMENTS

This work was supported by the Engineering and Physical Sciences Research Council [grant numbers EP/F064276/1, EP/K039911/1, EP/M001636/1, EP/N028260/1]; and the European

Commission [FP7-ICT project ID 611001]. Thanks are also extended to the numerous household inhabitants who have participated in the studies over the past 10 years. Data supporting this publication is not openly available, as University of Nottingham ethics approval does not allow for the release of transcripts containing personal data to third parties.

REFERENCES

1. Ackerman, M S, Cranor, L F and Reagle, J (1999) Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences, *Proceedings of E-COMMERCE 99*, New York; ACM, 1-8
2. Acquisti, A and Gross, R (2006) Imagined communities: Awareness, information sharing, and privacy on the Facebook, *Privacy Enhancing Technologies*, Springer
3. Al-Fedaghi, S (2007) How sensitive is your personal information?, *Proceedings of SAC'07*, ACM
4. Anderson, Jonathan, Claudia Diaz, Joseph Bonneau, and Frank Stajano. (2009) Privacy-enabling social networking over untrusted networks. In *Proceedings of the 2nd ACM workshop on Online social networks (WOSN '09)*. ACM, New York, NY, USA, 1-6.
5. Balebako, R, Jung, J, Lu, W, Cranor, L F and Nguyen, C (2013) "Little brothers watching you": raising awareness of data leaks on smartphones, *Proceedings of SOUPS '13*, New York: ACM
6. Barnes, S B (2006) A privacy paradox: Social networking in the Unites States, *First Monday*, Volume 11, No 9, 4 September 2006
7. Beach, S, Schulz, R, Downs, J, Matthews, J, Barron, B, and Seelman, K (2009) Disability, Age, and Informational Privacy Attitudes in Quality of Life Technology Applications: Results from a National Web Survey, *Transactions on Accessible Computing (TACCESS),* Volume 2 Issue 1, New York: ACM
8. Bellotti, V and Sellen, A (1993) Design for privacy in ubiquitous computing environments, *Proceedings of ECSCW '93*, Springer
9. Bonneau, Joseph, Jonathan Anderson, and George Danezis. (2009) "Prying data out of a social network." Social Network Analysis and Mining. *ASONAM'09. International Conference on Advances in. IEEE*.
10. Boyle, M and Greenberg, S (2005) The language of privacy: Learning from video media space analysis and design, *Transactions on Computer-Human Interaction (TOCHI),* Volume 12 Issue 2, New York: ACM
11. Brody et al (2012) *Social Networking and Impression Management: Self-Presentation in the Digital Age,* Lexington
12. Capra, R and Teevan, J (2012) Personal information management in a socially networked world, *Proceedings of CSCW'12*, New York: ACM
13. Chakraborty, S, Raghavan, K R, Johnson, M P and Srivastava, M B (2013) A framework for context-aware privacy of sensor data on mobile systems, *Proceedings of HotMobile'13*, New York: ACM
14. Chen, Y and Jones, G J F (2010) Augmenting human memory using personal lifelogs, *Proceedings of AH'10*, New York: ACM
15. Chen, Y and Xu, H (2013) Privacy management in dynamic groups: understanding information privacy in medical practices, *Proceedings of CSCW '13*, New York: ACM
16. Clarke, J, Castro, R R, Sharma, A, Lopez, J and Suri, N (2012) Trust & Security RTD in the internet of things: opportunities for international cooperation, *Proceedings of SecurIT'12*, New York: ACM
17. Crabtree, A., Rodden, T., Tolmie, P., Mortier, R., Lodge. T., Brundell, P. and Pantidi, N. (2014) "House rules: the collaborative nature of policy in domestic networks", Personal and Ubiquitous Computing, vol. 19 (1), pp. 203-215.
18. Crabtree, A. and Mortier, R. (2015) "Human data interaction: historical lessons from social studies and CSCW", Proceedings of the 14th European Conference on Computer Supported Cooperative Work, pp. 1-20, Oslo, Springer.
19. Crabtree, A. and Mortier, R. (2016) "Personal data, privacy and the Internet of Things: the shifting locus of agency and control", Social Science Research Network
20. Crabtree, A., Lodge, T., Colley, J., Greenhalgh, C., Mortier, R. and Haddadi, H. (2016) "Enabling the new economic actor: data protection, the digital economy, and the Databox", Personal and Ubiquitous Computing
21. Crabtree, A, Tolmie, P & Knight, W (2017) Repacking 'privacy' for a networked world, *to appear in* Proceedings of ECSCW '17, Springer
22. Donath, J and Boyd, D (2004) Public Displays of Connection, *BT Technology Journal*, October 2004, Volume 22, Issue 4, 71-82
23. Dourish, P., B. E. Grinter, J. D. D. L. Flor, and M. Joseph, (2004) "Security in the wild: User strategies for managing security as an everyday, practical problem," *Personal and Ubiquitous Computing*, vol. 8, no. 6, 2004.
24. Durrant, A, Golembewski, M, Kirk, D S, Beford, S, Rowland, D and McAuley, D (2011) Exploring a digital economy design space in theme parks, *Proceedings of DESIRE '11*, New York: ACM
25. Dwyer, C, Hiltz, S R, and Passerini, K (2007) Trust and Privacy Concern Within Social Networking Sites: A

Comparison of Facebook and MySpace, *AMCIS 2007*

26. Ellison, N B, Steinfield, C, Lampe, C (2007) The benefits of Facebook "friends". Social capital and college students' use of online social network sites, *Journal of Computer-Mediated Communication*, Wiley
27. Emanuel, L, Bevan C and Hodges, D (2013) What does your profile really say about you?: privacy warning systems and self-disclosure in online social network spaces, Proceedings of CHI EA '13, New York: ACM
28. Froehlich, J, Chen, M Y, Consolvo, S, Harrison, B, and Landay, J A (2007) MyExperience: a system for in situ tracing and capturing of user feedback on mobile phones, Proceedings of MobiSys'07, New York: ACM
29. Garfinkel, H. (1967) *Studies in Ethnomethodology*, Englewood Cliffs, Prentice-Hall.
30. Ghani, N A and Sidek, Z M (2008) Controlling your personal information disclosure, *Proceedings of ISP'08*, WSEAS
31. Goulden, M et al (2017) Living with Interpersonal Data: Observbility and Accountability in the Age of Pervasive ICT, to appear in *New Media and Society*
32. Greenberg, S and Rounding, M (2001) The notification collage: posting information to public and personal displays, *Proceedings of CHI'01*, New York: ACM, 514-521
33. Guha, S. and Wicker, S. (2015) "Do birds of a feather watch each other? Homophily and social surveillance in location-based social networks", *Proc. of CSCW*, pp. 1010-1020, Vancouver, ACM
34. Haddadi, H, Mortier, R, Hand, S, Brown, I, Yoneki, E, McAuley, D, Crowcroft, J (2012) Privacy analytics, *SIGCOMM Computer Communication Review*, Volume 42, Issue 3, New York: ACM
35. Hardt, Michaela and Suman Nath. (2012) Privacy-aware personalization for mobile advertising. In *Proceedings of the 2012 ACM conference on Computer and communications security (CCS '12)*. ACM, New York, NY, USA, 662-673.
36. Hawkey, K and Inkpen, K M (2006) Keeping up appearances: understanding the dimensions of incidental information privacy, *Proceedings of CHI '06*, New York: ACM
37. Hoffman, D L, Novak, T P and Peralta, M (1999) Building consumer trust online, *Communications of the ACM*, 1999
38. Hughes, J., King, V., Rodden, T., Andersen, H. (1994) 'Moving out of the control room: ethnography in system design', in *Proceedings of the Conference on Computer-Supported Cooperative Work (CSCW'94),* Chapel Hill: ACM Press, pp. 429-438
39. Joinson, A N (2008) Looking at, looking up or keeping up with people?: motives and use of Facebook, *Proceedings of CHI'08*, New York: ACM
40. Kaasten, S., Greenberg, S. and Edwards, C. How People Recognize Previously Seen WWW Pages from Titles, URLs and Thumbnails. In *Proc. of Human Computer Interaction 2002*, Springer Verlag (2002), 247-265.
41. Karr-Wisniewski, P., D. Wilson, and H. Richter-Lipford. (2011) A new social order: Mechanisms for social network site boundary regulation. In *AMCIS 2011 Proceedings, AMCIS '11*, page 9, Aug. 2011.
42. Kim, P, Podlaseck, M and Pingali, G (2004) Personal chronicling tools for enhancing information archival and collaboration in enterprises, *Proceedings of CARPE'04*, New York: ACM
43. Kirk, D S and Sellen, A (2010) On human remains: Values and practice in the home archiving of cherished objects, *Transactions on Computer-Human Interaction (TOCHI),* Volume 17 Issue 3, New York: ACM
44. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B.M., LeGrand, L., Powledge, P. and Wetherall, D. (2009) "When I am on Wi-Fi, I am Fearless:" Privacy Concerns & Practices in Everyday WiFi Use, *Proceedings of CHI 2009*, ACM
45. Krishnan, A and Jones, S (2005) TimeSpace: activity-based temporal visualisation of personal information spaces, *Personal and Ubiquitous Computing*, January 2005, Volume 9, Issue 1
46. Kwan, G C E and Skoric, M M (2013) Facebook bullying: An extension of battles in school, *Computers in Human Behavior*, Volume 29 Issue 1, Elsevier
47. Lampinen, A., S. Tamminen, and A. Oulasvirta. (2009) All my people right here, right now: management of group co-presence on a social networking site. In *Proceedings of the ACM 2009 international conference on Supporting group work, GROUP '09*, pages 281–290, New York, NY, USA, 2009. ACM.
48. Lenhart, A and Madden, M (2007) Teens, privacy & online social networks: How teens manage their online identities and personal information in the age of MySpace, Pew Internet & American Life Project
49. Li, I, Forlizzi, J and Dey, A (2010) Know thyself: monitoring and reflecting on facets of one's life, Proceedings of CHI EA'10, New York: ACM
50. Lin, J, Amini, S, Hong, J I, Sadeh, N, Lindqvist, J and Zhang, J (2012) Expectation and purpose: understanding users' mental models of mobile app privacy through crowdsourcing, *Proceedings of UbiComp '12*, New York: ACM
51. Livingstone, S (2008) Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression, *New Media & Society*, June 2008, vol. 10, no. 3, 393-411
52. Milberg, S J, Burke, S J, Smith, H J and Kallman, E A (1995) Values, personal information privacy, and regulatory

approaches, *Communications of the ACM*, Volume 38 Issue 12, Dec. 1995, 65-74

53. Morris, M E, Consolvo, S, Munson, S, Patrick, K, Tsai, J and Kramer, A D I (2011) Facebook for health: opportunities and challenges for driving behavior change, *Proceedings of CHI EA '11*, New York: ACM
54. Mortier, R et al (2010) The personal container, or your life in bits, *Proceedings of Digital Futures*
55. Mortier, R., H. Haddadi, T. Henderson, D. McAuley, J. Crowcroft (2013). Challenges & Opportunities in Human-Data Interaction. The Fourth Digital Economy All-hands Meeting: Open Digital (DE). November 4–6, 2013. Salford, UK
56. Multisilta, J and Milrad, M (2009) Sharing Experiences with Social Mobile Media, *Proceedings of MobileHCI'09,* New York: ACM
57. Murphy, M S (2011) Notes toward a politics of personalization, *Proceedings of iConference'11*, New York: ACM
58. Nath, S, Lin, F X, Ravindranath, L and Padhye, J (2013) SmartAds: bringing contextual ads to mobile apps, *Proceedings of MobiSys '13*, New York: ACM
59. Page, X., Knijnenburg, B. and Kobsa, A. (2013) "What a tangled web we weave: lying backfires in location-sharing social media", *Proc. of CSCW*, pp. 273-284, San Antonio, ACM.
60. Patil, S., Norcie, G, Kapadia, A and Lee, A.J. (2012) Reasons, Rewards, Regrets: Privacy Considerations in Location Sharing as an Interactive Practice, *Proceedings of the Symposium on Usable Privacy and Security (SOUPS) 2012*, ACM
61. Phelps, J, Nowak, G and Ferrell, E (2000) Privacy Concerns and Consumer Willingness to Provide Personal Information, *Journal of Public Policy & Marketing*, Vol. 19, No.1, (Spring, 2000), 27-41
62. Raij, A, Ghosh, A, Kumar, S and Srivastava, M (2011) Privacy risks emerging from the adoption of innocuous wearable sensors in the mobile environment, *Proceedings of CHI'11*, New York: ACM
63. Ryle, G. (1949) *The Concept of Mind*, London: Hutchinson.
64. Sacks, H. (1992) *Lectures on Conversation, Volumes I & II*, (edited by G. Jefferson), Malden, MA: Blackwell.
65. Schneier, Bruce, "A Taxonomy of Social Networking Data," *Security & Privacy, IEEE* , vol.8, no.4, pp.88, July-Aug. 2010.
66. Schrammel, J, Koffel, C and Tscheligi, M (2009) How much do you tell?: information disclosure behaviour in different types of online communities, *Proceedings of C&T '09*, New York: ACM
67. Sellen, A J, Fogg, A, Aitken, M, Hodges, S, Rother, C and Wood, K (2007) Do life-logging technologies support memory for the past?: an experimental study using sensecam, *Proceedings of CHI'07*, New York: ACM
68. Sheridan, J, Bryan-Kinns, N, Reeves, S, Marshall, J, and Lane, G (2011) Graffito: crowd-based performative interaction at festivals, *Proceedings of CHI '11 Extended Abstracts on Human Factors in Computing Systems (CHI EA '11)*, ACM: New York, 1129-1134
69. Sleeper, M, Cranshaw, J, Kelley, P G, Ur, B, Acquisti, A, Cranor, L F and Sadeh, N (2013) "I read my Twitter the next morning and was astonished": a conversational perspective on Twitter regrets, *Proceedings of CHI'13, New York: ACM*
70. Smale, S and Greenberg, S (2006) Transient life: collecting and sharing personal information, *Proceedings of OZCHI'06,* ACM
71. Song, J, Lee, S and Kim, J (2013) I know the shortened URLs you clicked on Twitter: inference attack using public click analytics and Twitter metadata, *Proceedings of WWW'13*, IWWWCSC
72. Stutzman F., and W. Hartzog. (2012) Boundary regulation in social media. In *Proceedings of ACM Conference on Computer Supported Cooperative Work, CSCW '12*, pages 769–778, Seattle, Washington, United States, 2012.
73. Tang, K.P., Hong, J.I., Siewiorek, D.P. (2011) Understanding how visual representations of location feeds affect end-user privacy concerns, *Proceedings of UbiComp '11*, New York: ACM
74. Taylor, C., and Dajani, L. (2008) The future of homecare systems in the context of the ubiquitous web and its related mobile technologies, *Proceedings of PETRA'08*, New York: ACM
75. Tolmie, P., Crabtree, A., Rodden, T., Colley, J. and Luger, E. (2016) "'This has to be the cats' - personal data legibility in networked sensing systems", Proceedings of the 19th Conference on Computer Supported Cooperative Work, pp. 491-502, San Francisco, ACM.
76. Viswanath, B., Emre Kiciman, and Stefan Saroiu. 2012. Keeping information safe from social networking apps. In *Proceedings of the 2012 ACM workshop on Workshop on online social networks (WOSN '12)*. ACM, New York, NY, USA, 49-54.
77. Wang, Y, Norcie, G, Komanduri, S, Acquisti, A, Leon, P G, and Cranor, L F (2011) "I regretted the minute I pressed share": a qualitative study of regrets on Facebook, Proceedings of SOUPS'11, New York: ACM
78. Watson, J. Besmer, A, Richter Lipford, H (2012) +Your Circles: Sharing Behavior on Google+, *Proceedings of Symposium on Usable Privacy and Security (SOUPS 2012*, ACM
79. Wisniewski, P., H. Lipford, and D. Wilson. (2012) Fighting for my space: Coping mechanisms for SNS boundary regulation. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems, CHI '12*, pages 609–618, New York, NY, USA, 2012. ACM

80. Zhao, S, Grasmuck, S and Martin, J (2008) Identity construction on Facebook: Digital empowerment in anchored relationships. *Computers in human behavior*, Elsevier